



Billing Code: 4410-13-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 02-2019]

Privacy Act of 1974; Systems of Records

AGENCY: Civil Rights Division, United States Department of Justice.

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Civil Rights Division (CRT), a component within the United States Department of Justice (DOJ or Department), proposes to develop a new system of records notice titled DOJ Insight Program Records System, JUSTICE/CRT-011. CRT proposes to establish this system of records to facilitate the Department's Insight Program, a training activity for DOJ attorneys to, among other tasks, gauge reaction and thought processing of DOJ-volunteers presented with proposed trial arguments.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The public, OMB, and Congress are invited to submit any comments by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, National Place Building, 1331 Pennsylvania Avenue, NW., Suite 1000, Washington, DC 20530; by facsimile at 202-307-0693; or by email at

privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Daniel Yi, Senior Counsel, Civil Rights Division, 950 Pennsylvania Avenue, NW, Washington DC 20530, phone: (202) 514-4609.

SUPPLEMENTARY INFORMATION:

In order to assist in achieving its mission and performance goals by improving employee and organizational performance, DOJ is authorized to develop training activities for its employees using a full range of options to meet its mission-related organizational and employee development needs. As such, the Department recognizes that trial attorneys faced with important questions and decisions for their juries and judges lack available resources to gauge reaction and thought processing when those individuals are presented with the DOJ attorneys' proposed arguments. Through the Insight Program, the Department believes it can assist and train its trial attorneys by leveraging a community of DOJ volunteers to review and provide feedback to proposed strategies and arguments.

The InSight Program will invite willing DOJ volunteers to participate in a community of virtual focus group panelists who are ready and willing to provide insights about certain DOJ cases. InSight will attempt to assemble a panel of DOJ volunteers that is similar to a trial attorney's jury and/or judge. The volunteer panelists will be provided case-related information and watch recorded videos of the DOJ attorney's anticipated strategy, and afterwards, will anonymously provide feedback to the DOJ attorney. The Justice Management Division (JMD) will provide technical resources and support to

facilitate the InSight Program, but CRT will retain manage and oversight of the InSight Program.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: June 3, 2019.

Peter A. Winn,
Acting Chief Privacy and Civil Liberties Officer,
United States Department of Justice.

JUSTICE/CRT-011**SYSTEM NAME AND NUMBER:**

DOJ Insight Program Records System, JUSTICE/CRT-011

SECURITY CLASSIFICATION:

Controlled Unclassified Information.

SYSTEM LOCATION:

Access to these electronic records includes all Department locations that the JMD or CRT operates, or that support CRT or JMD operations, including but not limited to, Two Constitution Square, 145 N Street NE, Washington, DC 20530. Some or all system information may also be duplicated at other locations where the Department has granted direct access to support CRT and JMD operations, system backup, emergency preparedness, and/or continuity of operations. To determine the location of particular records within the DOJ Insight Program Records System, contact the system manager, whose contact information is listed in the "SYSTEM MANAGER(S)" paragraph, below.

SYSTEM MANAGER(S):

Special Counsel for Innovation, Civil Rights Division, 950 Pennsylvania Avenue, NW, Washington DC 20530, phone: (202) 514-4609.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C § 4103, and 5 CFR part 410.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to facilitate the Department's Insight Program, a DOJ-developed training activity for DOJ attorneys to gauge reaction and thought processing of individuals presented with proposed trial arguments. This includes,

but is not limited to: providing Insight Program administrators with volunteer panelist information needed to assemble a panel similar to a DOJ trial attorney's jury and/or judge; allowing volunteer panelists to anonymously provide feedback to DOJ trial attorneys about proposed case strategies and presentations; allowing DOJ trial attorneys to use the feedback provided to refine strategies and arguments.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The Insight Program Records System collects and maintains information on DOJ employees who (1) administer the DOJ Insight Program; (2) volunteer as a DOJ Insight Program volunteer; or (3) otherwise request to participate in the DOJ Insight Program.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Insight Program Records System contains information on DOJ employees administering, participating in, or volunteering for the Insight Program. Such information includes, but is not limited to:

A. Basic participating information (for example, name, division, contact information, assigned Insight Program number, and signed consent forms) on DOJ Insight Program administrators, DOJ Insight Program volunteers, and DOJ trial attorneys participating in the DOJ Insight Program;

B. Background and attitudinal information on DOJ Insight Program volunteers;

C. Information used to facilitate DOJ trial attorneys' focal group requests (for example, criteria used to select the appropriate DOJ Insight Program volunteers, and case-relevant documents and video recordings of DOJ trial attorneys);

D. Tailored information, questionnaires, and feedback related to a DOJ trial attorney's focal group request; and

E. Insight Program information system user activity and audit logs.

RECORD SOURCE CATEGORIES:

Records contained in this system of records are derived from information provided directly by the DOJ employee or from the information system accessing the Insight Program Records System.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

A. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature – the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

B. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

C. To any person or entity that the [component/office] has reason to believe possesses information regarding a matter within the jurisdiction of the [component/office], to the extent deemed to be necessary by the [component/office] in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

F. To the news media and the public, including disclosures pursuant to 28 CFR § 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

G. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

H. To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would

occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

I. To appropriate officials and employees of a Federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

J. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

L. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

M. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the

Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

N. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach, or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

O. To any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of the Department and meeting related reporting requirements.

P. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in an electronic form in a framework of computer systems that allows distributed processing of data sets across clusters of computers. Records are stored securely in accordance with applicable executive orders, statutes, and agency implementing recommendations. Electronic records are stored in databases and/or on hard disks, removable storage devices, or other electronic media. Hard copies of records

may also be maintained in paper format, which will be stored in filing cabinets in a secure room.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by name or assigned Insight Program number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of as Department-wide legal and litigation training records, in accordance with the schedule approved by the Archivist of the United States, Job Number DAA-0060-2017-0009-0002.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Both electronic and paper records are safeguarded in accordance with appropriate laws, rules, and policies, including Department and CRT policies. The records are protected by physical security methods and dissemination/access controls. Direct access is controlled and limited to approved personnel with an official need for access to perform their duties. Paper files are stored: (1) in a secure room with controlled access; (2) in locked file cabinets; and/or (3) in other appropriate GSA approved security containers. Information systems and electronic records are protected by physical, technical, and administrative safeguards. Records are located in a building with restricted access and are kept in a locked room with controlled access or are safeguarded with approved encryption technology. The use of multifactor authentication is required to access electronic systems. Information may be transmitted to routine users on a need to know basis in a secure manner and to others upon verification of their authorization to access the information and their need to know. Internet connections are protected by

multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the Civil Rights Division FOIA/Privacy Act Branch, Patrick Henry Building, Room 9154, 601 D St. NW, Washington, DC 20579, *CRT.FOIArequests@usdoj.gov*. The envelope and letter should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request must include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Although no specific form is required, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice Web site at <https://www.justice.gov/oip/oip-request.html>.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR Part 16 Subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "RECORD ACCESS

PROCEDURES” paragraph, above. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked “Privacy Act Amendment Request.” All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

More information regarding the Department’s procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR §16.46, “Requests for Amendment or Correction of Records.”

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the “RECORD ACCESS PROCEDURES” paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2019-12152 Filed: 6/7/2019 8:45 am; Publication Date: 6/10/2019]